

Long-Distance Measurement-Device-Independent Multiparty Quantum Communication

Yao Fu,^{1,2} Hua-Lei Yin,^{1,2} Teng-Yun Chen,^{1,2} and Zeng-Bing Chen^{1,2,*}

¹*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

²*The CAS Center for Excellence in QIQP and the Synergetic Innovation Center for QIQP, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

(Dated: March 5, 2015)

The Greenberger-Horne-Zeilinger (GHZ) entanglement, originally introduced to uncover the extreme violation of local realism against quantum mechanics, is an important resource for multiparty quantum communication tasks. But the low intensity and fragility of the GHZ entanglement source in current conditions have made the practical applications of these multiparty tasks an experimental challenge. Here we propose a feasible scheme for practically distributing the post-selected GHZ entanglement over a distance of more than 100 km for experimentally accessible parameter regimes. Combining the decoy-state and measurement-device-independent protocols for quantum key distribution, we anticipate that our proposal suggests an important avenue for practical multiparty quantum communication.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Ac, 03.65.Ud

Remote distribution of quantum signals (photonic states) is an essential task in the realm of quantum communication. Quantum key distribution (QKD) allows the information-theoretically secure transmission of classical messages and requires delivery of either single photons in the case of BB84 protocol [1], or entangled photons in the case of Ekert91 protocol [2]. Remote distribution of entanglement also enables certain classically impossible tasks, such as quantum teleportation of unknown states and quantum dense coding [3]. Up to now, tremendous efforts have been dedicated to increase the transmission distance of quantum communication between *two* legitimate users. The recorded distance for QKD has been more than 300 km for standard telecom fiber links [4], while quantum teleportation has been demonstrated over a distance of more than 100 km for free-space channels [5].

So far, most theoretical and experimental works on quantum communication are focused on two-party protocols. Yet, multiparty quantum communication protocols do exist, as illustrated by the fascinating examples like quantum cryptographic conferencing (QCC) [4, 5], quantum secret sharing (QSS) [6, 9–11] and third-man quantum cryptography [12]. These multiparty protocols require an important resource—the Greenberger-Horne-Zeilinger (GHZ) entangled states [13, 33] with perfect multiparty quantum correlations, which are originally introduced to reveal the extreme violation of local realism against quantum mechanics. Nevertheless, the practical applications of GHZ states are quite limited due to the lack of two important factors—the high-intensity source and remote reliable distribution of the GHZ states. The existing experimental works [10] on multiparty quantum communication remain the proof-of-principle demonstration and reported rather low key rates. The experimental

distribution of the GHZ entanglement [15] was achieved only recently, over a distance of less than 1 km for each party of the GHZ-entangled photons. Thus, the current status of multiparty quantum communication still remains an extreme experimental challenge even under the state-of-the-art technologies and is far from practical applications. In this Letter, we propose a feasible scheme for distributing the post-selected GHZ entanglement over a distance of more than 100 km for experimentally relevant parameter regimes. Combining the decoy-state QKD [16] and the measurement-device-independent (MDI) QKD [17] technologies, our findings manifest the possibility for practical applications of MDI multiparty quantum communication such as QCC and QSS, as well as for the long-distance GHZ experiment.

Multiparty quantum communication protocols aim to provide information-theoretic security for highly sensitive and confidential multiuser communication based on the laws of quantum mechanics, which physically outperform their classical counterparts. Their applications [6, 9, 11] range from the secret multiparty conference, remote voting, online auctioning, master key of the payment system, jointly checking accounts containing quantum money [18], to secure distributed quantum computation [19]. Among them, QCC is a protocol for multiparty QKD [5], which requires a common random bit sequence (the keys) to be securely shared among the legitimate users even in the presence of any eavesdropper. QSS is a protocol of splitting a message into several parts amongst a group of participants, each of whom is allocated a share of the secret [6]. As a consequence, only the entire set is sufficient to read the message thoroughly. For example, QSS can be used to guarantee that no single person can launch a nuclear missile, or open a bank vault, but all legitimate users together can.

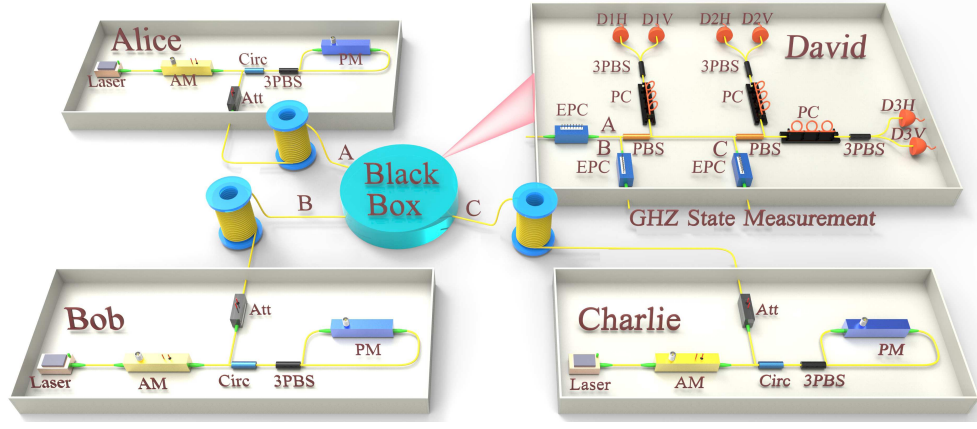


FIG. 1. (color online) Schematic layout of the MDI-QCC setup. AM: amplitude modulator used to prepare decoy states; 3PBS: 3-port polarization-maintaining PBS, which, besides the function of PBS, can transit optical pulses from fast axis to slow axis; Circ: circulator; PM: phase modulator, combining with 3PBS and Circ, is used to encode qubits; PC: polarization controller which makes a unitary transformation like a half-wave plate such that it corresponds to a 45° rotation of the polarization; Black Box: the GHZ-state measurement device; Att: attenuator used to prepare weak coherent pulses; EPC: electric polarization controller used to adjust the frame of reference; PBS: polarizing beam-splitter which transmits $|H\rangle$ and reflects $|V\rangle$ polarizations; D1H, D2V, D2H D2V, D3H and D3V: single-photon detectors.

Before we describe our multiparty communication schemes in detail, let us recapitulate the significance of the GHZ state $|\Phi_0^\pm\rangle = 1/\sqrt{2}(|HHH\rangle \pm |VVV\rangle)$, where $|H\rangle$ and $|V\rangle$ represent photonic horizontal and vertical polarizations, respectively. If three members of a GHZ state are measured along Z basis, each of them will give a random outcome, Z_A , Z_B , Z_C , and the outcomes of the three members will always be in perfect correlations, $Z_A = Z_B = Z_C$, which can be used for multiparty quantum cryptographic conferencing. Likewise, when three members of a GHZ state $|\Phi_0^+\rangle$ ($|\Phi_0^-\rangle$) are measured along X basis, each will give a random outcome i.e., X_A , X_B , X_C , whose sharing of a binary correlation $X_A = X_B \oplus X_C$ ($X_A \oplus 1 = X_B \oplus X_C$) will always hold and can then be used for multiparty QSS. Besides, when Alice announces her measurement result X_A , Bob and Charlie will have a perfect correlation which can be used for third-man quantum cryptography.

Here we exploit an approach that requires neither the preparation in advance nor the distribution of high-fidelity GHZ entangled states through a long distance. The design is to take advantage of post-selected GHZ states among three legitimate users (typically called Alice, Bob and Charlie) to perform information-theoretically secure multiparty quantum communication. Like the MDI-QKD protocol [17], the post-selecting measurement device here can be regarded as a black box which can be manipulated by anyone, even the eavesdropper. Therefore, our scheme is naturally immune to all detection-side attacks and can be regarded as the combination of time-reversed GHZ state distribution and measurement. Together with the decoy-state method [16], in which pulses with different amplitudes are randomly

mixed and phases are randomized, our scheme is able to defeat photon-number-splitting attacks [20]. We utilize conventional laser sources to obtain a long distribution distance between the middle node and users for both the MDI-QCC and MDI-QSS protocols. Similarly to the security proof of QKD [17, 21], we use multiparty entanglement purification technique [22] to provide information-theoretically secure information transmission. The security of our protocols is analyzed in the Supplemental Material [23].

In the following, let us explain our MDI-QCC and MDI-QSS protocols in more details. The main quantum procedures of the two schemes are the same, while the difference lies in their classical post-processing. The MDI-QCC (MDI-QSS) protocol uses the data in Z (X) basis to extract secure keys. Our setup is depicted in Fig. 1. Here, we take MDI-QCC protocol as an example. Alice, Bob and Charlie independently and randomly prepare quantum states with phase-randomized weak coherent pulses in two complementary bases (Z basis and X basis). They send the pulses to the untrusted fourth-party located in the middle node, David, to perform a GHZ-state measurement which projects the incoming signals onto a GHZ state. Such a measurement can be realized, for instance, using only linear optical elements [12]. Actually, this procedure only identifies two of the eight GHZ states, while the identification of any one GHZ state is enough to prove the security. A successful GHZ-state measurement corresponds to the observation of three out of six detectors being clicked simultaneously. The clicks in D1H, D2H and D3H, or in D1H, D2V and D3V, or in D1V, D2H and D3V, or in D1V, D2V and D3H, imply a projection onto the GHZ state $|\Phi_0^+\rangle = 1/\sqrt{2}(|HHH\rangle + |VVV\rangle)$,

while the clicks in D1H, D2H and D3V, or in D1H, D2V and D3H, or in D1V, D2H and D3H, or in D1V, D2V and D3V, indicate a projection onto the GHZ state $|\Phi_0^-\rangle = 1/\sqrt{2}(|HHH\rangle - |VVV\rangle)$. David announces the events through public channels whether he has obtained a GHZ state and which GHZ state he has received. Alice, Bob and Charlie only keep the raw data of successful GHZ-state measurements and discard the rest. They post-select the events where they use the same basis in their transmission through an authenticated public channel. Notice that Alice performs a bit flip when Alice, Bob and Charlie all choose X basis and David obtains a GHZ state $|\Phi_0^-\rangle$. We employ the data of Z basis to generate the cryptographic conferencing keys, while the data of X basis are totally used to estimate errors. Alice, Bob and Charlie estimate the gain and quantum bit error rate with decoy-state method, given that all of them send out single-photon states. Afterwards, they extract secure cryptographic conferencing keys after classical error correction and privacy amplification.

In the asymptotic limit, the MDI-QCC key generation rate is given by [17, 20, 22]

$$R_{QCC} = Q_v^Z + Q_{111}^Z[1 - H(e_{111}^{BX})] - H(E_{\mu\nu\omega}^{Z*})fQ_{\mu\nu\omega}^Z, \quad (1)$$

where $Q_{\mu\nu\omega}^Z$ ($E_{\mu\nu\omega}^{Z*}$), the gain (quantum bit error rate) of Z basis, can be directly obtained from the experimental results. The subscript $\mu\nu\omega$ means that Alice, Bob and Charlie send out phase-randomized weak coherent pulses with intensity μ , ν and ω , respectively. Note that each of these pulses has single-photon state components and the ones of n (> 1) photons or zero photon. For the post-selected GHZ states contributed solely by the single-photon state components, the gain Q_{111}^Z of Z basis and the bit error rate e_{111}^{BX} of X basis can be estimated by the decoy-state method. Q_v^Z is the gain that Alice sends out vacuum state component in Z basis and David obtains a GHZ state measurement result. Here, we assume that Alice's raw key is the reference raw key, the parameter f is the error correction efficiency ($f = 1.16$ in our simulation below), and $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary Shannon entropy function. The information-theoretic security proof of MDI-QCC is shown in the Supplemental Material, from which we have $E_{\mu\nu\omega}^{Z*} = \max\{E_{\mu\nu\omega}^{ZAB}, E_{\mu\nu\omega}^{ZAC}\}$. Here, $E_{\mu\nu\omega}^{ZAB}$ ($E_{\mu\nu\omega}^{ZAC}$) is the quantum bit error rate of Z basis between Alice and Bob (Charlie).

In the same manner, the key generation rate of MDI-QSS in the asymptotic limit is given by

$$R_{QSS} = Q_v^X + Q_{111}^X[1 - H(e_{111}^{BZ})] - H(E_{\mu\nu\omega}^X)fQ_{\mu\nu\omega}^X, \quad (2)$$

where $Q_{\mu\nu\omega}^X$ ($E_{\mu\nu\omega}^X$), the gain (quantum bit error rate) of X basis, can also be directly obtained from the experimental results. For the single-photon state contribution, the gain Q_{111}^X of X basis and bit error rate e_{111}^{BZ} of Z basis can be estimated by the decoy-state method. Q_v^X

is the gain that Alice sends out vacuum state component in X basis and David obtains a GHZ state measurement result. However, the overall quantum bit error rate $E_{\mu\nu\omega}^X$ (always about 37.5% for arbitrarily-long transmission distances) in X basis is so high that it is virtually impossible to use weak coherent sources to perform MDI-QSS with Eq. (2). To solve the problem, in the Supplemental Material we propose, in details, to use the triggered spontaneous parametric down conversion sources [32], or the conventional weak coherent state sources together with the quantum non-demolition measurement technique [36].

However, such a solution is disadvantageous as it requires experimentally challenging technology. Fortunately, we can exploit the extra classical bit information [22, 31] to extract the raw key with little bit error rate (almost zero) so that we can implement MDI-QSS, again with weak coherent sources. The classical bit information corresponds to the information denoted by different overall phase regions over $[0, 2\pi)$ (the phase post-selection technique). Meanwhile, we assume the gain and bit error rate of single-photon states to be in a uniform distribution over $[0, 2\pi)$ [22]. Therefore, the secure key rate of MDI-QSS with phase post-selection can be given by (see Supplemental Material [23] for details)

$$\tilde{R}_{QSS} \geq \frac{1}{K^2} Q_{111}^X[1 - H(e_{111}^{BZ})] - H(\tilde{E}_{\mu\nu\omega}^X)f\tilde{Q}_{\mu\nu\omega}^X, \quad (3)$$

where K is the number of phase regions, $\tilde{Q}_{\mu\nu\omega}^X$ and $\tilde{E}_{\mu\nu\omega}^X$ are the gain and bit error rate of the pulses whose information is used to extract the raw key with little bit error rate. The phase post-selection technique requires to share a common phase reference [39] among users. A method for distributing such a phase reference is suggested in Supplemental Material [23]. We note that the rigorous security of protocols involving phase post-selection technique needs more investigations in the contexts of both QKD [22, 31] and MDI-QSS.

To analyze the performance of the secret key rates of MDI-QCC and MDI-QSS, we present an analytical method with two decoy states to estimate the relevant parameters Q_{111}^Z , Q_{111}^X , e_{111}^{BZ} and e_{111}^{BX} , which are required to be evaluated in Eqs. (1)-(37). In our simulation, we employ the following experimental parameters: the intrinsic loss coefficient β of the standard telecom fiber channel is 0.2 dB/km. For the threshold single-photon detectors, the detection efficiency $\eta_d = 40\%$, and the background count rate $p_d = 1 \times 10^{-7}$, as used in a recent decoy-state MDI-QKD experiment [40]. As a comparison, we also use the state-of-the-art single-photon detectors [41], with $\eta_d = 93\%$ and $p_d = 1 \times 10^{-7}$. Here, we neglect the overall misalignment-error probability of the system. The secure key rates of MDI-QCC with weak coherent sources in the cases of infinite decoy states and of the two decoy states are shown in Fig. 2a. From the simu-

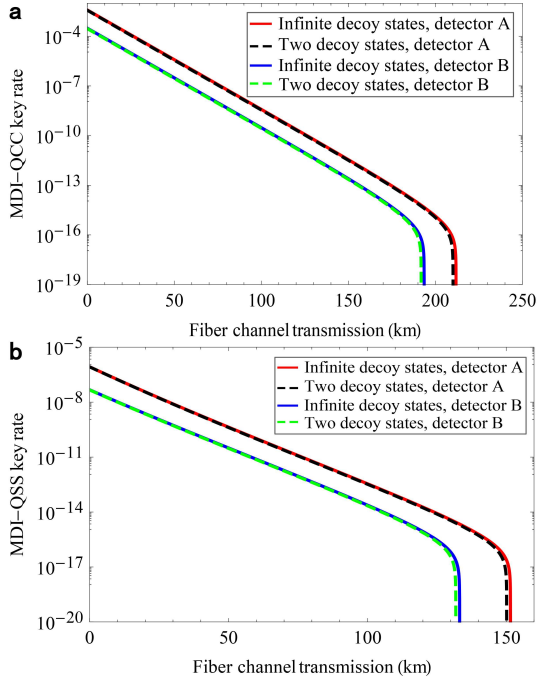


FIG. 2. (color online) Lower bound on the secure key rates versus fiber channel transmission. **a**, MDI-QCC with weak coherent sources. **b**, MDI-QSS with weak coherent sources based on phase post-selection technique ($K = 8$). We show the simulation results of infinite decoy states and two decoy states with detector A (B) of detection efficiency 93% (40%), respectively. The phase-randomized weak coherent sources with (without) the phase post-selection technique are used for MDI-QSS (MDI-QCC). The intensity of the signal state and one decoy state is 0.4 and 0.005 (0.11 and 0.005), while the other decoy state is a vacuum state in MDI-QCC (MDI-QSS).

lation result, we see that the estimation using two decoy states gives a secure key rate which is nearly the same as the corresponding one using infinite decoy states. In the case of asymptotic data with two decoy states, the secure transmission distance between Alice and the middle node of MDI-QCC is about 190 km for the detection efficiency of 40% (210 km for the detection efficiency of 93%). The secure key rates of MDI-QSS with weak coherent sources based on overall phase post-selection technique are shown in Fig. 2b. In the case of asymptotic data with two decoy states, the secure transmission distance is about 130 km for the detection efficiency of 40% (150 km for the detection efficiency of 93%) between the middle node and any user.

The information-theoretic security of our multiparty quantum communication protocols is guaranteed by the GHZ entanglement purification technique [22] though the security of MDI-QSS is complicated by phase post-selection and needs further study. Indeed, the purpose of QCC and QSS protocols can be recognized as a procedure for Alice, Bob and Charlie to share almost perfect

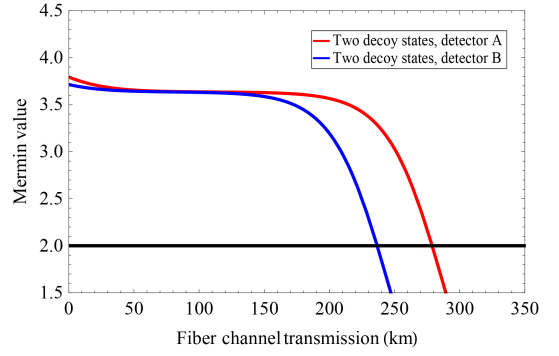


FIG. 3. (color online) The Mermin value M_{111} versus fiber channel transmission. We use two decoy states to estimate M_{111} . We show the simulation results for detector A (B) of detection efficiency of 93% (40%) in red (blue) solid curve, respectively, the overall misalignment-error probability e_d of the system is 1.5%, with other parameters identical to Fig. 2a. We also show the line of constant 2, which is the maximal value allowed by local realism.

GHZ states. Qualitatively, the more perfect the GHZ entanglement shared by Alice, Bob and Charlie is, the more negligible the information would have been leaked to Eve [9]. It is thus of vital importance to quantify the quality of the GHZ entanglement. For this purpose, Alice, Bob and Charlie independently and randomly prepare quantum states with phase-randomized weak coherent pulses in two complementary bases (X basis and Y basis) and then send to David, who performs the GHZ-state ($|\Phi_0^+\rangle$) measurement. What we take into consideration here is the post-selected GHZ states contributed solely by the single-photon state components. This contribution can be estimated by the decoy-state method. For the GHZ entangled state $|\Phi_0^+\rangle$, local realistic theories must obey Mermin's inequality [33]:

$$M_{111} \equiv \langle XXX \rangle_{111} - \langle XYY \rangle_{111} - \langle YXY \rangle_{111} - \langle YYX \rangle_{111} \leq 2. \quad (4)$$

Here M_{111} is defined as the Mermin value and witnesses the quality of the GHZ entanglement; $\langle XXX \rangle_{111}$ and so on are the expectation values with respect to the GHZ states solely contributed by the single-photon state components. It is important to ensure that one only selects a single ensemble corresponding to the successful projection onto the GHZ state $|\Phi_0^+\rangle$. In our post-selected GHZ states, the Mermin value, whose maximal value is 4 as predicted by quantum mechanics for ideal GHZ states, can reach about 3.5 as shown in Fig. 3 over the distribution distance of about 170 km from David to Alice (Bob, Charlie); more details can be found in the Supplemental Material [23]. This indicates that high-quality GHZ entanglement can be generated at this distance by the protocol. The proposed protocol can be regarded as a variance of the usual GHZ experiment testing local realism, namely, a time-reversed GHZ experiment where the state

preparations replace the state measurements in the usual GHZ test. The interpretation of such a variance and, particularly, its relevance to the test of hidden-variable theories are interesting in its own right. We argue in the Supplemental Material [23] that such an experiment tests Mermin's argument [35] on the Kochen-Specker theorem [34].

In summary, we propose a feasible protocol for distributing the post-selected GHZ entanglement and MDI multiparty quantum communication over a distance of more than 100 km for experimentally accessible parameter regimes. Combining the decoy-state and MDI protocols for QKD, we show that the information-theoretically secure MDI-QCC with the conventional weak coherent state sources can be implemented over a distance of about 190 km, as well as the MDI-QSS with weak coherent sources based on phase post-selection technique over a distance of about 130 km. These distances are significantly beyond what one could expect previously for multiparty quantum communication with the GHZ entanglement. Our proposal thus suggests an important avenue for practical long-distance multiparty quantum communication. The extension of our scheme to more legitimate users is straightforward.

We are grateful to the anonymous Referees for their valuable comments and suggestions to improve the quality of the paper. This work has been supported by the CAS, the NNSF of China under Grant No. 61125502, and the Science Fund of Anhui Province for Outstanding Youth. Y.F. and H.-L.Y. contributed equally to this work.

* zbchen@ustc.edu.cn

- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
- [2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [3] J.-W. Pan *et al.*, Rev. Mod. Phys. **84**, 777 (2012).
- [4] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).
- [5] J. Yin *et al.*, Nature (London) **488**, 185 (2012). X.-S. Ma *et al.*, Nature (London) **489**, 269 (2012).
- [6] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
- [7] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).
- [8] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
- [9] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
- [10] W. Tittel *et al.*, Phys. Rev. A **63**, 042301 (2001). Y.-A. Chen *et al.*, Phys. Rev. Lett. **95**, 200502 (2005). S. Gaertner *et al.*, Phys. Rev. Lett. **98**, 020503 (2007). C. Schmid *et al.*, Phys. Rev. Lett. **95**, 230505 (2005).
- [11] B. Bell *et al.*, Nat. Commun. **5**, 5480 (2014).
- [12] M. Żukowski *et al.*, Acta Phys. Pol. **93**, 187 (1998).
- [13] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (edited by M. Kafatos,) (Kluwer Academic, Dordrecht, 1989), pp. 69–72.
- [14] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [15] C. Erven *et al.*, Nat. Photon. **8**, 292 (2014).
- [16] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003). H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005). X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012). S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
- [18] S. Wiesner, SIGACT News **15**, 78 (1983).
- [19] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
- [20] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
- [21] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999). P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000). H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
- [22] E. N. Maneva *et al.*, Contemp. Math. **305**, 203 (2002). C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996). W. Dür *et al.*, Phys. Rev. Lett. **83**, 3562 (1999).
- [23] See Supplemental Material, which includes Refs. [24–32].
- [24] C.-Y. Lu, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **103**, 020501 (2009).
- [25] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).
- [26] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
- [27] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
- [28] S.-B. Cho *et al.*, Opt. Express **17**, 19027 (2009). Y. Liu *et al.*, Phys. Rev. Lett. **109**, 030501 (2012). A. Cuevas *et al.*, Nat. Commun. **4**, 2871 (2013).
- [29] T. Scheidl *et al.*, Proc. Natl. Acad. Sci. **107**, 19708 (2010).
- [30] Z.-B. Chen *et al.*, Phys. Rev. Lett. **90**, 160408 (2003).
- [31] A. Peres, J. Mod. Opt. **47**, 139 (2000).
- [32] X.-S. Ma *et al.*, Nature Phys. **8**, 479 (2012).
- [33] J.-W. Pan and A. Zeilinger, Phys. Rev. A **57**, 2208 (1998).
- [34] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
- [35] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
- [36] P. Grangier *et al.*, Nature (London) **396**, 537 (1998). A. Mizutani *et al.*, Sci. Rep. **4**, 5236 (2014).
- [37] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).
- [38] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
- [39] J. M. Arrazola *et al.*, Phys. Rev. A **89**, 062305 (2014). J. M. Arrazola *et al.*, Phys. Rev. A **90**, 042335 (2014). V. Dunjko *et al.*, Phys. Rev. Lett. **112**, 040502 (2014).
- [40] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
- [41] F. Marsili *et al.*, Nat. Photon. **7**, 210 (2013).
- [42] B. M. Terhal, IBM J. Research and Development **48**, 71 (2004).
- [43] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
- [44] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).

**SUPPLEMENTAL MATERIAL FOR “LONG DISTANCE MEASUREMENT-DEVICE-INDEPENDENT
MULTIPARTY QUANTUM COMMUNICATION”**

I. SECURITY ANALYSIS

A. GHZ State Entanglement Purification

Here, the goal of an entanglement purification protocol is to distill nearly perfect GHZ states from noisy GHZ states initially shared among three distant parties (typically called Alice, Bob and Charlie). The density matrix ρ_{ABC} describing Alice, Bob and Charlie's qubit system can be expressed in the GHZ basis [1], which is composed of eight orthogonal GHZ states:

$$\begin{aligned}
 |\Phi_0^+\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle + |V\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++\rangle + |+-\rangle + |-+-\rangle + |--\rangle), \\
 |\Phi_0^-\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle - |V\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++\rangle + |+-\rangle + |-+-\rangle + |--\rangle), \\
 |\Psi_1^+\rangle &= \frac{1}{\sqrt{2}}(|V\rangle|H\rangle|H\rangle + |H\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++\rangle + |+-\rangle - |-+-\rangle - |--\rangle), \\
 |\Psi_1^-\rangle &= \frac{1}{\sqrt{2}}(|V\rangle|H\rangle|H\rangle - |H\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++\rangle + |+-\rangle - |-+-\rangle - |--\rangle), \\
 |\Psi_2^+\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle|H\rangle + |V\rangle|H\rangle|V\rangle) = \frac{1}{2}(|++\rangle - |+-\rangle + |-+-\rangle - |--\rangle), \\
 |\Psi_2^-\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle|H\rangle - |V\rangle|H\rangle|V\rangle) = \frac{1}{2}(|++\rangle - |+-\rangle + |-+-\rangle - |--\rangle), \\
 |\Psi_3^+\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|V\rangle + |V\rangle|V\rangle|H\rangle) = \frac{1}{2}(|++\rangle - |+-\rangle - |-+-\rangle + |--\rangle), \\
 |\Psi_3^-\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|V\rangle - |V\rangle|V\rangle|H\rangle) = \frac{1}{2}(|++\rangle - |+-\rangle - |-+-\rangle + |--\rangle).
 \end{aligned} \tag{5}$$

We take $|\Phi_0^+\rangle$ as the reference state in this paper. The GHZ state $|\Phi_0^+\rangle$ is stabilized by its stabilizer generators, i.e.,

$$S_0 = XXX, \quad S_1 = ZZI, \quad S_2 = ZIZ, \tag{6}$$

where

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{7}$$

denote the phase shift, bit flip and no operation acting on the qubit, respectively. Maneva and Simolin [2] proposed a multiparty hashing protocol to distill nearly perfect GHZ states by generalizing the quantum XOR operation used in Ref. [3] to the case of multiparty setting. The yield (per input mixed state) in the case of asymptotic data is given by [2]

$$D_h = 1 - \max\{H(e_{b_1}), H(e_{b_2})\} - H(e_p). \tag{8}$$

Here $H(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the standard binary Shannon entropy function, e_p is the phase shift error rate corresponding to the stabilizer generator S_0 , while e_{b_1} and e_{b_2} represent the bit flip error rates corresponding to the stabilizer generator S_1 and S_2 , respectively. One can choose two (classical) random hashing codes, one of which is used to correct bit flip errors and the other one is used to correct phase errors. This can be done by local operation and classical communication with the help of multilateral quantum XOR operations.

Consider the tripartite density matrix ρ_{ABC} which describes the qubit system of Alice, Bob and Charlie [1, 4]

$$\begin{aligned}
 \rho_{ABC} &= \lambda_1 |\Phi_0^+\rangle \langle \Phi_0^+| + \lambda_2 |\Phi_0^-\rangle \langle \Phi_0^-| + \lambda_3 |\Psi_1^+\rangle \langle \Psi_1^+| + \lambda_4 |\Psi_1^-\rangle \langle \Psi_1^-| \\
 &\quad + \lambda_5 |\Psi_2^+\rangle \langle \Psi_2^+| + \lambda_6 |\Psi_2^-\rangle \langle \Psi_2^-| + \lambda_7 |\Psi_3^+\rangle \langle \Psi_3^+| + \lambda_8 |\Psi_3^-\rangle \langle \Psi_3^-|,
 \end{aligned} \tag{9}$$

where $\sum_{i=1}^8 \lambda_i = 1$. $e_{b_1}^Z$ and $e_{b_2}^Z$ are defined as the bit flip error rates between Alice and Bob's bits and between Alice and Charlie's bits in Z basis corresponding to the stabilizer generator S_1 and S_2 , respectively, which can be obtained

from Eq. (5) and Eq. (9) as,

$$\begin{aligned} e_{b_1}^Z &= \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6, \\ e_{b_2}^Z &= \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8. \end{aligned} \quad (10)$$

We employ the bit error rate e_b^Z to represent the probability that all the bit values of Alice, Bob and Charlie are not the same,

$$e_b^Z = \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8. \quad (11)$$

The phase shift error rate corresponding to the stabilizer generator S_0 in Z basis can be given by

$$e_p^Z = \lambda_2 + \lambda_4 + \lambda_6 + \lambda_8. \quad (12)$$

Furthermore, if Alice, Bob and Charlie measure the GHZ state in X basis, the random measurement outcomes will always share a binary correlation $X_A = X_B \oplus X_C$. The bit flip error rate in X basis is the probability of $X_A \oplus 1 = X_B \oplus X_C$, while the phase shift error rate in X basis is the probability that the relative phase changes. $X_A \in \{0, 1\}$ is the binary data corresponding to the polarization $\{|+\rangle, |-\rangle\}$ of Alice. Therefore, from Eq. (5) and Eq. (9), the bit flip error rate and phase shift error rate in X basis can be given by

$$\begin{aligned} e_b^X &= \lambda_2 + \lambda_4 + \lambda_6 + \lambda_8 = e_p^Z, \\ e_p^X &= \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 = e_b^Z. \end{aligned} \quad (13)$$

B. Post-selected GHZ States

Entanglement purification of GHZ states are closely related to multiparty communication protocols, such as quantum cryptographic conferencing (QCC) [4, 5] and quantum secret sharing (QSS) [6–8]. The relation between them is that if Alice, Bob and Charlie share almost perfect pure GHZ states, the states will be nearly unentangled with Eve's system, which is the term *monogamy of entanglement* [9]. Therefore, the information leaked to Eve is negligible, and Alice, Bob and Charlie can obtain an information-theoretically secure key by measuring the GHZ states. Thus, the purpose of QCC and QSS protocols can be recognized as a procedure for Alice, Bob and Charlie to share almost perfect GHZ states, which is also the purpose of the entanglement purification protocol. Entanglement purification protocol can be transformed into the quantum error correction protocol [3], while Calderbank-Shor-Steane (CSS) code can be used to prove the security of quantum communication protocols [10, 11]. With the important property of CSS code, the error correction procedure for the phase shift error will be decoupled from the error correction procedure for the bit flip error. The quantum error correction can be transformed into classical post-processing, the bit error correction (phase error correction) can be regarded as the classical error correction (privacy amplification).

We use a GHZ-state analyzer [12] to post-select GHZ states among three legitimate users (Alice, Bob and Charlie). The events can be regarded as the time-reversed GHZ state distribution and measurement. Similar to the security proof of measurement-device-independent (MDI) quantum key distribution [10, 13, 14], we suppose that each of Alice, Bob and Charlie has an Einstein-Podolsky-Rosen entangled state which contains one virtual qubit in each of them and the other qubit is sent to the middle node, David. When David performs a successful GHZ-state measurement, the virtual qubit of the legitimate users becomes a GHZ-entangled state, the procedure of which can be then regarded as a multiparty entanglement swapping, as experimentally demonstrated [15]. Alice, Bob and Charlie can utilize quantum memory to store their virtual qubits. After David announces the events through public channels whether he has obtained a GHZ state and which GHZ state he has received, Alice, Bob and Charlie will measure their virtual qubits. According to different multiparty quantum communication protocols such as the QCC, QSS and third-man quantum cryptography, the legitimate users perform the corresponding operations to classical post-processing. They can extract secure keys after the processes of basis sift, error correction and privacy amplification, which are all classical procedures. Combined with the decoy state method [16–18], some practical sources can be used in our schemes for multiparty quantum communication. For instance, weak coherent sources emitted by laser diodes are used in MDI-QCC, weak coherent states with extra classical bit information (the phase post-selection technique) are used in MDI-QSS. Meanwhile, heralded single-photon sources (also called triggered spontaneous parametric down conversion sources) are used in MDI-QSS. Furthermore, we exploit the quantum non-demolition measurement technique [19] to effectively realize a long distribution distance MDI-QSS with weak coherent sources.

II. MDI-QUANTUM CRYPTOGRAPHIC CONFERENCING

When the phases of the weak coherent pulses sent by Alice, Bob and Charlie are fully randomized, the density matrix of the coherent states can be written as

$$\rho_1 = \int_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta} \sqrt{\mu}\rangle \langle e^{i\theta} \sqrt{\mu}| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n|, \quad (14)$$

where θ and μ are the phase and intensity of the coherent states, respectively. Then the quantum channel can be considered as a photon number channel [17]. Note that the multi-photon components are tagged ones whose information will be fully leaked to Eve [20], the secure key rate of MDI-QCC can be given by

$$R_{QCC} = Q_v^Z + Q_{111}^Z [1 - H(e_{111}^{PZ})] - \max \{H(E_{\mu\nu\omega}^{ZAB}), H(E_{\mu\nu\omega}^{ZAC})\} f Q_{\mu\nu\omega}^Z, \quad (15)$$

where $Q_{111}^Z = \mu\nu\omega e^{-\mu-\nu-\omega} Y_{111}^Z$ is the gain of the single-photon states in Z basis, $Q_v^Z = e^{-\mu} Q_{0\nu\omega}^Z$ is the gain that Alice sends out vacuum state component in Z basis and David obtains a GHZ state measurement result. Here, we assume that Alice's raw key is the reference raw key. For single-photon states, the phase error probability e_{111}^{PZ} in Z basis is equal to the bit error probability e_{111}^{BX} in X basis in the case of asymptotic data according to Eq. (13), i.e., $e_{111}^{PZ} = e_{111}^{BX}$. $Q_{\mu\nu\omega}^Z$ is the overall gain in Z basis and f is the error correction efficiency. $E_{\mu\nu\omega}^{ZAB}$ ($E_{\mu\nu\omega}^{ZAC}$) is the bit flip error rate between Alice's and Bob's (Charlie's) bits in Z basis.

In the following, we will focus on the evolution of the joint quantum states before they enter the detectors. Due to the basis sift in the classical post-processing, we only discuss the case of ZZZ and XXX . The joint quantum states of Alice, Bob and Charlie sending out horizontal polarization weak coherent states can be given by

$$|e^{i\phi_a} \sqrt{\mu}\rangle_H |e^{i\phi_b} \sqrt{\nu}\rangle_H |e^{i\phi_c} \sqrt{\omega}\rangle_H, \quad (16)$$

where ϕ_a , ϕ_b and ϕ_c are the overall randomized phases. Then the quantum states arriving at David's GHZ state measurement device (before the quantum states enter the detectors) are given by

$$|e^{i\phi_b} \sqrt{\frac{\nu\eta_b}{2}}\rangle_{1H} |e^{i\phi_b} \sqrt{\frac{\nu\eta_b}{2}}\rangle_{1V} |e^{i\phi_c} \sqrt{\frac{\omega\eta_c}{2}}\rangle_{2H} |e^{i\phi_c} \sqrt{\frac{\omega\eta_c}{2}}\rangle_{2V} |e^{i\phi_a} \sqrt{\frac{\mu\eta_a}{2}}\rangle_{3H} |e^{i\phi_a} \sqrt{\frac{\mu\eta_a}{2}}\rangle_{3V}, \quad (17)$$

where the six detection modes are $1H$, $1V$, $2H$, $2V$, $3H$ and $3V$, respectively. η_a , η_b , η_c are the overall detection efficiencies of Alice, Bob and Charlie, respectively. Therefore, the detection probabilities for the six threshold single-photon detectors can be written as

$$\begin{aligned} D_{1H} = D_{1V} &= 1 - (1 - p_d) \exp\left(-\frac{\nu\eta_b}{2}\right), \quad D_{2H} = D_{2V} = 1 - (1 - p_d) \exp\left(-\frac{\omega\eta_c}{2}\right), \\ D_{3H} = D_{3V} &= 1 - (1 - p_d) \exp\left(-\frac{\mu\eta_a}{2}\right). \end{aligned} \quad (18)$$

The gain $Q_{HHH}^{\mu\nu\omega\Phi_0^+}$ is defined as the probability that Alice, Bob and Charlie send out horizontal polarization weak coherent states with the intensity of μ , ν and ω , respectively, with David obtaining a successful GHZ state $|\Phi_0^+\rangle$ measurement event, which is given by

$$\begin{aligned} Q_{HHH}^{\mu\nu\omega\Phi_0^+} &= \frac{1}{8} [D_{1H} D_{2H} D_{3H} (1 - D_{1V})(1 - D_{2V})(1 - D_{3V}) + D_{1H} D_{2V} D_{3V} (1 - D_{1V})(1 - D_{2H})(1 - D_{3H}) \\ &\quad + D_{1V} D_{2H} D_{3V} (1 - D_{1H})(1 - D_{2V})(1 - D_{3H}) + D_{1V} D_{2V} D_{3H} (1 - D_{1H})(1 - D_{2H})(1 - D_{3V})], \\ &= \frac{1}{2} (1 - p_d)^3 e^{-\frac{x}{2}} \left[1 - (1 - p_d) e^{-\frac{\mu\eta_a}{2}}\right] \left[1 - (1 - p_d) e^{-\frac{\nu\eta_b}{2}}\right] \left[1 - (1 - p_d) e^{-\frac{\omega\eta_c}{2}}\right], \end{aligned} \quad (19)$$

where $x = \mu\eta_a + \nu\eta_b + \omega\eta_c$, $1/8$ stands for the probability of a $|HHH\rangle$ polarization when Alice, Bob and Charlie all choose Z basis, p_d is the background count rate. Due to symmetry, we have

$$Q_{HHH}^{\mu\nu\omega\Phi_0^+} = Q_{HHH}^{\mu\nu\omega\Phi_0^-} = Q_{VVV}^{\mu\nu\omega\Phi_0^+} = Q_{VVV}^{\mu\nu\omega\Phi_0^-} = A. \quad (20)$$

According to the above procedures, we have

$$\begin{aligned} Q_{HHV}^{\mu\nu\omega\Phi_0^+} &= Q_{HVV}^{\mu\nu\omega\Phi_0^+} = Q_{HHV}^{\mu\nu\omega\Phi_0^-} = Q_{HVV}^{\mu\nu\omega\Phi_0^-} = \frac{p_d}{2} (1 - p_d)^3 e^{-x} \left(1 - p_d - e^{-\frac{\nu\eta_b}{2}}\right) \left(1 - p_d - e^{\frac{1}{2}(\mu\eta_a + \omega\eta_c)} I_0(\sqrt{\mu\eta_a \omega\eta_c})\right) = B, \\ Q_{VHH}^{\mu\nu\omega\Phi_0^+} &= Q_{VHV}^{\mu\nu\omega\Phi_0^+} = Q_{VHH}^{\mu\nu\omega\Phi_0^-} = Q_{VHV}^{\mu\nu\omega\Phi_0^-} = \frac{p_d}{2} (1 - p_d)^3 e^{-x} \left(1 - p_d - e^{-\frac{\omega\eta_c}{2}}\right) \left(1 - p_d - e^{\frac{1}{2}(\mu\eta_a + \nu\eta_b)} I_0(\sqrt{\mu\eta_a \nu\eta_b})\right) = C, \\ Q_{HVH}^{\mu\nu\omega\Phi_0^+} &= Q_{V VH}^{\mu\nu\omega\Phi_0^+} = Q_{HVH}^{\mu\nu\omega\Phi_0^-} = Q_{V VH}^{\mu\nu\omega\Phi_0^-} = \frac{p_d}{2} (1 - p_d)^3 e^{-x} \left(1 - p_d - e^{-\frac{\mu\eta_a}{2}}\right) \left(1 - p_d - e^{\frac{1}{2}(\nu\eta_b + \omega\eta_c)} I_0(\sqrt{\nu\eta_b \omega\eta_c})\right) = D, \end{aligned} \quad (21)$$

where $I_0(x)$ is the modified Bessel function of the first kind.

In the same manner, when Alice, Bob and Charlie all choose X basis, we have

$$\begin{aligned} Q_{+++}^{\mu\nu\omega\Phi_0^+} &= Q_{+--}^{\mu\nu\omega\Phi_0^+} = Q_{-+-}^{\mu\nu\omega\Phi_0^+} = Q_{--+}^{\mu\nu\omega\Phi_0^+} = Q_{++-}^{\mu\nu\omega\Phi_0^-} = Q_{+-+}^{\mu\nu\omega\Phi_0^-} = Q_{-++}^{\mu\nu\omega\Phi_0^-} = Q_{---}^{\mu\nu\omega\Phi_0^-} = E, \\ Q_{+++}^{\mu\nu\omega\Phi_0^-} &= Q_{+--}^{\mu\nu\omega\Phi_0^-} = Q_{-+-}^{\mu\nu\omega\Phi_0^-} = Q_{--+}^{\mu\nu\omega\Phi_0^-} = Q_{++-}^{\mu\nu\omega\Phi_0^+} = Q_{+-+}^{\mu\nu\omega\Phi_0^+} = Q_{-++}^{\mu\nu\omega\Phi_0^+} = Q_{---}^{\mu\nu\omega\Phi_0^+} = F, \end{aligned} \quad (22)$$

and

$$\begin{aligned} Q_{+++}^{\mu\nu\omega\Phi_0^+} &= \frac{1}{8} \int_0^{2\pi} \int_0^{2\pi} [F_{1H}F_{2H}F_{3H}(1-F_{1V})(1-F_{2V})(1-F_{3V}) + F_{1H}F_{2V}F_{3V}(1-F_{1V})(1-F_{2H})(1-F_{3H}) \\ &\quad + F_{1V}F_{2H}F_{3V}(1-F_{1H})(1-F_{2V})(1-F_{3H}) + F_{1V}F_{2V}F_{3H}(1-F_{1H})(1-F_{2H})(1-F_{3V})] \frac{d\phi}{2\pi} \frac{d\varphi}{2\pi}, \\ Q_{+++}^{\mu\nu\omega\Phi_0^-} &= \frac{1}{8} \int_0^{2\pi} \int_0^{2\pi} [F_{1H}F_{2H}F_{3V}(1-F_{1V})(1-F_{2V})(1-F_{3H}) + F_{1H}F_{2V}F_{3H}(1-F_{1V})(1-F_{2H})(1-F_{3V}) \\ &\quad + F_{1V}F_{2H}F_{3H}(1-F_{1H})(1-F_{2V})(1-F_{3V}) + F_{1V}F_{2V}F_{3V}(1-F_{1H})(1-F_{2H})(1-F_{3H})] \frac{d\phi}{2\pi} \frac{d\varphi}{2\pi}, \end{aligned} \quad (23)$$

where F_{1H} is the detection probability of detection mode $1H$, $\phi = \phi_a - \phi_b$, $\varphi = \phi_a - \phi_c$, and

$$\begin{aligned} F_{1H} &= 1 - (1-p_d)e^{-\left(\frac{\mu\eta_a + \nu\eta_b}{4} + \frac{\sqrt{\mu\eta_a\nu\eta_b}}{2} \cos \phi\right)}, \quad F_{1V} = 1 - (1-p_d)e^{-\left(\frac{\mu\eta_a + \nu\eta_b}{4} - \frac{\sqrt{\mu\eta_a\nu\eta_b}}{2} \cos \phi\right)}, \\ F_{2H} &= 1 - (1-p_d)e^{-\left(\frac{\nu\eta_b + \omega\eta_c}{4} + \frac{\sqrt{\nu\eta_b\omega\eta_c}}{2} \cos(\varphi - \phi)\right)}, \quad F_{2V} = 1 - (1-p_d)e^{-\left(\frac{\nu\eta_b + \omega\eta_c}{4} - \frac{\sqrt{\nu\eta_b\omega\eta_c}}{2} \cos(\varphi - \phi)\right)}, \\ F_{3H} &= 1 - (1-p_d)e^{-\left(\frac{\mu\eta_a + \omega\eta_c}{4} + \frac{\sqrt{\mu\eta_a\omega\eta_c}}{2} \cos \varphi\right)}, \quad F_{3V} = 1 - (1-p_d)e^{-\left(\frac{\mu\eta_a + \omega\eta_c}{4} - \frac{\sqrt{\mu\eta_a\omega\eta_c}}{2} \cos \varphi\right)}. \end{aligned} \quad (24)$$

The overall gain and quantum bit error rates in Z basis can be given by

$$\begin{aligned} Q_{\mu\nu\omega}^Z &= Q_{\mu\nu\omega}^{CZ} + Q_{\mu\nu\omega}^{EZ} = Q_{\mu\nu\omega}^{CZAB} + Q_{\mu\nu\omega}^{EZAB} = Q_{\mu\nu\omega}^{CZAC} + Q_{\mu\nu\omega}^{EZAC} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} Y_{nml}^Z, \\ E_{\mu\nu\omega}^{EZ} Q_{\mu\nu\omega}^Z &= e_d Q_{\mu\nu\omega}^{CZ} + (1-e_d) Q_{\mu\nu\omega}^{EZ} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} e_{nml}^{BZ} Y_{nml}^Z, \\ E_{\mu\nu\omega}^{EZAB} Q_{\mu\nu\omega}^Z &= e_d Q_{\mu\nu\omega}^{CZAB} + (1-e_d) Q_{\mu\nu\omega}^{EZAB}, \quad E_{\mu\nu\omega}^{ZAC} Q_{\mu\nu\omega}^Z = e_d Q_{\mu\nu\omega}^{CZAC} + (1-e_d) Q_{\mu\nu\omega}^{EZAC}, \end{aligned} \quad (25)$$

where $E_{\mu\nu\omega}^Z$ is defined as the probability that all the bit values of Alice, Bob and Charlie are not the same in Z basis. Y_{nml}^Z (e_{nml}^{BZ}) is the yield (bit error rate) in Z basis, given that Alice, Bob and Charlie send out n -photon, m -photon and l -photon pulses, respectively. $Q_{\mu\nu\omega}^{CZ}$ ($Q_{\mu\nu\omega}^{EZ}$) is the total gain of a successful GHZ state measurement when the polarization of the pulses sent by Alice, Bob and Charlie are the same (different) in Z basis, which represents a correct (false) measurement result. $Q_{\mu\nu\omega}^{CZAB}$ ($Q_{\mu\nu\omega}^{EZAB}$) is the total gain of a successful GHZ state measurement when the polarization of the pulses sent by Alice and Bob are the same (different) in Z basis, which represents a correct (false) measurement result. $Q_{\mu\nu\omega}^{CZAC}$ ($Q_{\mu\nu\omega}^{EZAC}$) is the total gain of a successful GHZ state measurement when the polarization of the pulses sent by Alice and Charlie are the same (different) in Z basis, which represents a correct (false) measurement result. e_d represents the overall misalignment-error probability of the system. Therefore, we have

$$\begin{aligned} Q_{\mu\nu\omega}^{CZ} &= 4A, \quad Q_{\mu\nu\omega}^{EZ} = 4(B+C+D), \quad Q_{\mu\nu\omega}^{CZAB} = 4A+2B+2D, \\ Q_{\mu\nu\omega}^{EZAB} &= 2B+4C+2D, \quad Q_{\mu\nu\omega}^{CZAC} = 4A+2C+2D, \quad Q_{\mu\nu\omega}^{EZAC} = 4B+2C+2D. \end{aligned} \quad (26)$$

The overall gain $Q_{\mu\nu\omega}^X$ and quantum bit error rate $E_{\mu\nu\omega}^X$ in X basis can be given by

$$\begin{aligned} Q_{\mu\nu\omega}^X &= Q_{\mu\nu\omega}^{CX} + Q_{\mu\nu\omega}^{EX} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} Y_{nml}^X, \\ E_{\mu\nu\omega}^X Q_{\mu\nu\omega}^X &= e_d Q_{\mu\nu\omega}^{CX} + (1-e_d) Q_{\mu\nu\omega}^{EX} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} e_{nml}^{BX} Y_{nml}^X, \end{aligned} \quad (27)$$

where Y_{nml}^X (e_{nml}^{BX}) is the yield (bit error rate) in X basis, given that Alice, Bob and Charlie send out n -photon, m -photon and l -photon pulses, respectively. $Q_{\mu\nu\omega}^{CX}$ ($Q_{\mu\nu\omega}^{EX}$) is the total gain of a successful GHZ state measurement

when the correlation $X_A = X_B \oplus X_C$ ($X_A \oplus 1 = X_B \oplus X_C$) holds in X basis, which represents a correct (false) measurement result. Thus, we have $Q_{\mu\nu\omega}^{CX} = 8E$, $Q_{\mu\nu\omega}^{EX} = 8F$. Notice that Alice performs a bit flip when Alice, Bob and Charlie all choose X basis and David obtains the GHZ state $|\Phi_0^-\rangle$.

For simplicity, we consider a symmetric scenario that the distances L from Alice, Bob and Charlie to the middle node David are all the same. So $\eta_a = \eta_b = \eta_c = \eta_d \times 10^{-\beta L/10}$ is the overall efficiency including the channel transmission efficiency $10^{-\beta L/10}$ (β is the intrinsic loss coefficient of the standard telecom fiber channel and L is the distance between the legitimate users and David) and the efficiency of the detectors η_d . We present an analytical estimation method with two decoy states (vacuum+decoy state), here $\mu_2 = \nu_2 = \omega_2 > \mu_1 = \nu_1 = \omega_1 > 0$. With the derivation method mentioned in [21], we can calculate the lower bound of Y_{111}^{ZL} , Y_{111}^{XL} and the upper bound of e_{111}^{BXU} , e_{111}^{BZU} , which are given by

$$Y_{111}^{ZL} \geq \frac{1}{\mu_2^3 \mu_1^3 (\mu_2 - \mu_1)} \left[\mu_2^4 \left(e^{3\mu_1} Q_{\mu_1\mu_1\mu_1}^Z - e^{2\mu_1} Q_{\mu_1\mu_1 0}^Z - e^{2\mu_1} Q_{\mu_1 0\mu_1}^Z - e^{2\mu_1} Q_{0\mu_1\mu_1}^Z + e^{\mu_1} Q_{\mu_1 00}^Z \right. \right. \\ \left. \left. + e^{\mu_1} Q_{0\mu_1 0}^Z + e^{\mu_1} Q_{00\mu_1}^Z - Q_{000}^Z \right) - \mu_1^4 \left(e^{3\mu_2} Q_{\mu_2\mu_2\mu_2}^Z - e^{2\mu_2} Q_{\mu_2\mu_2 0}^Z \right. \right. \\ \left. \left. - e^{2\mu_2} Q_{\mu_2 0\mu_2}^Z - e^{2\mu_2} Q_{0\mu_2\mu_2}^Z + e^{\mu_2} Q_{\mu_2 00}^Z + e^{\mu_2} Q_{0\mu_2 0}^Z + e^{\mu_2} Q_{00\mu_2}^Z - Q_{000}^Z \right) \right], \quad (28)$$

$$Y_{111}^{XL} \geq \frac{1}{\mu_2^3 \mu_1^3 (\mu_2 - \mu_1)} \left[\mu_2^4 \left(e^{3\mu_1} Q_{\mu_1\mu_1\mu_1}^X - e^{2\mu_1} Q_{\mu_1\mu_1 0}^X - e^{2\mu_1} Q_{\mu_1 0\mu_1}^X - e^{2\mu_1} Q_{0\mu_1\mu_1}^X + e^{\mu_1} Q_{\mu_1 00}^X \right. \right. \\ \left. \left. + e^{\mu_1} Q_{0\mu_1 0}^X + e^{\mu_1} Q_{00\mu_1}^X - Q_{000}^X \right) - \mu_1^4 \left(e^{3\mu_2} Q_{\mu_2\mu_2\mu_2}^X - e^{2\mu_2} Q_{\mu_2\mu_2 0}^X \right. \right. \\ \left. \left. - e^{2\mu_2} Q_{\mu_2 0\mu_2}^X - e^{2\mu_2} Q_{0\mu_2\mu_2}^X + e^{\mu_2} Q_{\mu_2 00}^X + e^{\mu_2} Q_{0\mu_2 0}^X + e^{\mu_2} Q_{00\mu_2}^X - Q_{000}^X \right) \right], \quad (29)$$

$$e_{111}^{BXU} \leq \frac{1}{\mu_1^3 Y_{111}^{XL}} \left(e^{3\mu_1} E_{\mu_1\mu_1\mu_1}^X Q_{\mu_1\mu_1\mu_1}^X - e^{2\mu_1} E_{\mu_1\mu_1 0}^X Q_{\mu_1\mu_1 0}^X - e^{2\mu_1} E_{\mu_1 0\mu_1}^X Q_{\mu_1 0\mu_1}^X - e^{2\mu_1} E_{0\mu_1\mu_1}^X Q_{0\mu_1\mu_1}^X \right. \\ \left. + e^{\mu_1} E_{\mu_1 00}^X Q_{\mu_1 00}^X + e^{\mu_1} E_{0\mu_1 0}^X Q_{0\mu_1 0}^X + e^{\mu_1} E_{00\mu_1}^X Q_{00\mu_1}^X - E_{000}^X Q_{000}^X \right). \quad (30)$$

$$e_{111}^{BZU} \leq \frac{1}{\mu_1^3 Y_{111}^{ZL}} \left(e^{3\mu_1} E_{\mu_1\mu_1\mu_1}^Z Q_{\mu_1\mu_1\mu_1}^Z - e^{2\mu_1} E_{\mu_1\mu_1 0}^Z Q_{\mu_1\mu_1 0}^Z - e^{2\mu_1} E_{\mu_1 0\mu_1}^Z Q_{\mu_1 0\mu_1}^Z - e^{2\mu_1} E_{0\mu_1\mu_1}^Z Q_{0\mu_1\mu_1}^Z \right. \\ \left. + e^{\mu_1} E_{\mu_1 00}^Z Q_{\mu_1 00}^Z + e^{\mu_1} E_{0\mu_1 0}^Z Q_{0\mu_1 0}^Z + e^{\mu_1} E_{00\mu_1}^Z Q_{00\mu_1}^Z - E_{000}^Z Q_{000}^Z \right). \quad (31)$$

III. MDI-QUANTUM SECRET SHARING

A. MDI-QSS with Phase Post-selection Technique

The MDI-QCC (MDI-QSS) protocol uses the data in Z (X) basis to extract secure key. Thus, the secure key rate of MDI-QSS can be given by

$$R_{QSS} = Q_v^X + Q_{111}^X [1 - H(e_{111}^{PX})] - Q_{\mu\nu\omega}^X fH(E_{\mu\nu\omega}^X). \quad (32)$$

where $Q_{111}^X = \mu\nu\omega e^{-\mu-\nu-\omega} Y_{111}^X$. In the case of asymptotic data, for single-photon states, the phase error probability in X basis is equal to the bit error probability in Z basis according to Eq. (13), i.e., $e_{111}^{PX} = e_{111}^{BZ}$. $Q_v^X = e^{-\mu} Q_{0\nu\omega}^X$ is the gain that Alice sends out vacuum state component in X basis and David obtains a GHZ state measurement result. $Q_{\mu\nu\omega}^X$ ($E_{\mu\nu\omega}^X$) is the overall gain (bit error rate) in X basis, which can be directly obtained from the experimental results. Due to that the three parties send out vacuum state, single-photon state and two-photon state in X basis, respectively, David also obtains a GHZ state measurement result and the probability is the same order with that all the three parties send out single-photon states, i.e., $Q_{111}^X/2 \sim Q_{012}^X \sim Q_{021}^X \sim Q_{102}^X \sim Q_{120}^X \sim Q_{201}^X \sim Q_{210}^X \gg Q_{ijk}^X$ for $i+j+k > 3$. Therefore, the overall bit error rate in X basis can be written as

$$E_{\mu\nu\omega}^X \sim \frac{6e_{012} Q_{012}^X}{Q_{111}^X + 6Q_{012}^X} = 37.5\%, \quad (33)$$

where $e_{012} = 50\%$ since the vacuum state carries no bit information. However, the overall quantum bit error rate in X basis is so high that it is virtually impossible to use weak coherent sources to perform MDI-QSS with Eq. (32). Fortunately, we can exploit the extra classical bit information [22] to extract the raw key with little bit error rate (almost zero) so that we can implement the MDI-QSS with weak coherent sources. With the decoy state method [16–18], the overall phase are randomized over $[0, 2\pi)$, which can be divided into K parts in the following form

$$[0, 2\pi) = \bigcup_{k=0}^{K-1} \left\{ \left[\frac{k\pi}{K}, \frac{(k+1)\pi}{K} \right) \cup \left[\pi + \frac{k\pi}{K}, \pi + \frac{(k+1)\pi}{K} \right) \right\}. \quad (34)$$

Different regions can be denoted by classical bit information, for example, 3-bit classical information represents $K = 8$ phase regions. At the same time that Alice, Bob and Charlie announce their basis, they also announce their overall phase regions. Note that different overall phase regions correspond to different bit error rates, they can extract the raw key with little bit error rate according to phase bit information. Only when their phase regions are chosen the same, the bit error rates will reach the minimum value. Alice, Bob and Charlie only choose the data in the phase region $[0, \frac{\pi}{K}) \cup [\pi, \pi + \frac{\pi}{K})$ as the effective raw key. Thus, the gain and bit error rate of post-selection raw key can be written as

$$\tilde{Q}_{\mu\nu\omega}^X = \tilde{Q}_{\mu\nu\omega}^{CX} + \tilde{Q}_{\mu\nu\omega}^{EX}, \quad \tilde{E}_{\mu\nu\omega}^X \tilde{Q}_{\mu\nu\omega}^X = (1 - e_d) \tilde{Q}_{\mu\nu\omega}^{EX} + e_d \tilde{Q}_{\mu\nu\omega}^{CX}, \quad (35)$$

where

$$\begin{aligned} \tilde{Q}_{\mu\nu\omega}^{CX} &= \frac{K}{\pi^3} \int_0^{\frac{\pi}{K}} \int_0^{\frac{\pi}{K}} \int_0^{\frac{\pi}{K}} [F_{1H} F_{2H} F_{3H} (1 - F_{1V})(1 - F_{2V})(1 - F_{3V}) + F_{1H} F_{2V} F_{3V} (1 - F_{1V})(1 - F_{2H})(1 - F_{3H}) \\ &\quad + F_{1V} F_{2H} F_{3V} (1 - F_{1H})(1 - F_{2V})(1 - F_{3H}) + F_{1V} F_{2V} F_{3H} (1 - F_{1H})(1 - F_{2H})(1 - F_{3V})] d\phi_a d\phi_b d\phi_c, \\ \tilde{Q}_{\mu\nu\omega}^{EX} &= \frac{K}{\pi^3} \int_0^{\frac{\pi}{K}} \int_0^{\frac{\pi}{K}} \int_0^{\frac{\pi}{K}} [F_{1H} F_{2H} F_{3V} (1 - F_{1V})(1 - F_{2V})(1 - F_{3H}) + F_{1H} F_{2V} F_{3H} (1 - F_{1V})(1 - F_{2H})(1 - F_{3V}) \\ &\quad + F_{1V} F_{2H} F_{3H} (1 - F_{1H})(1 - F_{2V})(1 - F_{3V}) + F_{1V} F_{2V} F_{3V} (1 - F_{1H})(1 - F_{2H})(1 - F_{3H})] d\phi_a d\phi_b d\phi_c. \end{aligned} \quad (36)$$

We assume the gain and bit error rate of single-photon states to be in a uniform distribution over $[0, 2\pi)$ [22]. Therefore, the secure key rate of MDI-QSS with phase post-selection can be given by

$$\tilde{R}_{QSS} \geq \frac{1}{K^2} Q_{111}^X [1 - H(e_{111}^{BZ})] - H(\tilde{E}_{\mu\nu\omega}^X) f \tilde{Q}_{\mu\nu\omega}^X, \quad (37)$$

where $1/K^2$ represents the probability that all users select the same phase region and we neglect the contribution of vacuum state component that Alice sends out.

In practical experiments, the phase of the transferred signal will drift due to, e.g., temperature and mechanical stress variations on the optical fiber or air disturbance of the free-space channel. Fortunately, the drift of phase will not influence the results of our work, except for MDI-QSS with phase post-selection technique. The common phase reference is thus required to be shared among all users so that the users can tell which phase region they are. We remark that solving the problem of sharing common phase reference is to tackle long distance phase-stabilization, which is usually difficult and required also in quantum fingerprinting [23] and quantum digital signatures [24, 25].

Here, we suggest a possible way to implement phase compensation over a distance to enable the distribution of the common phase reference among all users. Alice, Bob and Charlie exploit continuous-wave laser sources with the same central wavelength and narrow line-width to generate continuous-wave laser with almost stabilized phases. The amplitude modulator generates reference light and signal light. The reference light is used for phase compensation, while the signal light is used for encoding qubits. When three reference lights with positive 45° polarization and same intensity enter the GHZ-analyzer, the GHZ-analyzer will unambiguously reveal whether the phases among them are the same or not [26], i.e., detector D1H and D1V compare the phases between Alice and Bob, detector D2H and D2V compare the phases between Bob and Charlie, detector D3H and D3V compare the phases between Alice and Charlie, respectively. Thus, with the detection results corresponding to reference light, one can realize the phase compensation, resulting in a common phase reference among all users. Considering the scattering effects in fiber, the reference light should not be too strong, so as to reduce the detrimental scattering effects. Another approach could be to use wavelength division multiplexing with the frequency of reference light less than that of signal light so that the detrimental scattered photons can be filtered out. As seen from Fig. 1 in the Supplemental Material of Ref [27], practically the phase drift is about 30π per second for 100 km standard single-mode fiber (SMF-28), so rapid feedback

algorithm is necessary for implementing long distance phase compensation. There are some rapid feedback algorithms realizing phase-stabilization for several kilometers [28–30]. However, successfully accomplishing long distance (100 km) phase-stabilization is still challenging under current technology.

It should be noted that the inclusion of phase post-selection complicates the security analysis, as pointed out in the context of device-independent QKD [31] or MDI-QKD [22]. The rigorous security of MDI-QSS with weak coherent states and phase post-selection thus needs more investigations, too.

B. MDI-QSS with Heralded Single-photon Sources

Except for the phase post-selection technique, we propose another two methods to perform MDI-QSS: the triggered spontaneous parametric down conversion sources, or the conventional weak coherent state sources together with the quantum non-demolition measurement technique. Instead of taking advantage of weak coherent states which are divided into two independent states after passing through a beam splitter, we use another universal method to process the joint quantum state evolution, which can also be used for any photon-number distribution (including coherent states) of the sources. That is, we use the heralded single-photon sources (also called triggered spontaneous parametric down-conversion sources) to perform MDI-QSS. Similarly to the above symmetric scenario, $\eta = \eta_a = \eta_b = \eta_c = \eta_d \times 10^{-\beta L/10}$. The quantum states coming from the heralded single-photon sources can be written as

$$|\Psi\rangle = (\cosh \chi^{-1}) \sum_{n=0}^{\infty} (\tanh \chi)^n |n, n\rangle. \quad (38)$$

We assume that the intensity of the sources is given by $\mu = \sinh^2 \chi$ and the heralded single-photon sources always send out photon pairs. Therefore, the photon number of two modes are always the same. The probability to get an n -photon pair is

$$P(n) = \frac{\mu^n}{(1 + \mu)^{n+1}}. \quad (39)$$

After triggering out one of the photon pairs, the density matrix of the other mode after phase randomization can then be given by [32]

$$\rho_2 = \frac{1}{P_c} \sum_{n=0}^{\infty} \frac{\mu^n}{(1 + \mu)^{n+1}} [1 - (1 - p_d)(1 - \eta_d)^n] |n\rangle\langle n| = \sum_{n=0}^{\infty} P_n(\mu) |n\rangle\langle n|, \quad (40)$$

where $P_c = (\mu\eta_d + p_d)/(1 + \mu\eta_d)$ is the post-selection probability given that one triggered mode leads to the click of the threshold single-photon detector.

We consider the joint quantum states when Alice and Bob send out i -photon and j -photon states with horizontal polarization, respectively, while Charlie sends out k -photon state with vertical polarization. The joint quantum states can be written as

$$|\Psi\rangle_{in}^{HHV} = |n\rangle_H |m\rangle_H |l\rangle_V = \frac{(a_{1H}^\dagger)^n}{\sqrt{n!}} \frac{(a_{2H}^\dagger)^m}{\sqrt{m!}} \frac{(a_{3V}^\dagger)^l}{\sqrt{l!}} |0\rangle. \quad (41)$$

The joint quantum states before entering the detectors can be given by

$$|\Psi\rangle_{out}^{HHV} = \sum_{p=0}^{n+l} \sum_{s=0}^m \sum_{t=0}^l \frac{(-1)^{l-t} C_n^{p-t} C_m^s C_l^t}{\sqrt{2^{n+m+l} n! m! l!}} \sqrt{p! s! (n+l-p)! (m-s)! (l-t)!} |s\rangle_{1H} |m-s\rangle_{1V} |0\rangle_{2H} |0\rangle_{2V} |p\rangle_{3H} |n+l-p\rangle_{3V}, \quad (42)$$

where $|\Psi\rangle_{out}^{HHV}$ denotes the superpositions of orthogonal states $|s\rangle_{1H} |m-s\rangle_{1V} |0\rangle_{2H} |0\rangle_{2V} |p\rangle_{3H} |n+l-p\rangle_{3V}$. Therefore, the gain $Q_{HHV}^{\mu\nu\omega\Phi_0^+}$ and the yield $Y_{nml}^{HHV\Phi_0^+}$ can be written as

$$\begin{aligned} Q_{HHV}^{\mu\nu\omega\Phi_0^+} &= \frac{1}{8} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} P_\mu(n) P_\nu(m) P_\omega(l) Y_{nml}^{HHV\Phi_0^+}, \\ Y_{nml}^{HHV\Phi_0^+} &= \sum_{p=0}^{n+l} \sum_{s=0}^m [G_{1H} G_{2H} G_{3H} (1 - G_{1V}) (1 - G_{2V}) (1 - G_{3V}) + G_{1H} G_{2V} G_{3V} (1 - G_{1V}) (1 - G_{2H}) (1 - G_{3H}) \\ &\quad + G_{1V} G_{2H} G_{3V} (1 - G_{1H}) (1 - G_{2V}) (1 - G_{3H}) + G_{1V} G_{2V} G_{3H} (1 - G_{1H}) (1 - G_{2H}) (1 - G_{3V})] P_{nml}^{HHV}, \end{aligned} \quad (43)$$

where P_{nml}^{HHV} is the probability of obtaining the quantum state $|s\rangle_{1H}|m-s\rangle_{1V}|0\rangle_{2H}|0\rangle_{2V}|p\rangle_{3H}|n+l-p\rangle_{3V}$, G_{1H} is the detection probability of detector mode $1H$, and

$$P_{nml}^{HHV} = \left| \sum_{t=0}^l \frac{(-1)^{l-t} C_n^{p-t} C_m^s C_l^t}{\sqrt{2^{n+m+l} n! m! l!}} \sqrt{p! s! (n+l-p)! (m-s)!} \right|^2, \quad (44)$$

$$G_{1H} = 1 - (1 - p_d)(1 - \eta)^s, \quad G_{1V} = 1 - (1 - p_d)(1 - \eta)^{m-s}, \quad G_{2H} = p_d,$$

$$G_{2V} = p_d, \quad G_{3H} = 1 - (1 - p_d)(1 - \eta)^p, \quad G_{3V} = 1 - (1 - p_d)(1 - \eta)^{n+l-p}.$$

The above methods can also be extended to cases of other polarizations.

Combining Eqs. (25), (26), (27) with Eq. (40), we will obtain $Q_{\mu\mu\mu}^X$ and $E_{\mu\mu\mu}^X$ under the heralded single-photon sources. Similar to Eqs. (28), (29), (30), we can obtain the lower bound of Y_{111}^{XL} , Y_{111}^{ZL} and the upper bound of e_{111}^{BZU} ,

$$Y_{111}^{XL} \geq \frac{1}{P_1^2(\mu_2)P_1^2(\mu_1)[P_2(\mu_2)P_1(\mu_1) - P_2(\mu_1)P_1(\mu_2)]} \left[P_1^2(\mu_2)P_2(\mu_2) \left(Q_{\mu_1\mu_1\mu_1}^X - P_0(\mu_1)Q_{\mu_1\mu_10}^X - P_0(\mu_1)Q_{\mu_10\mu_1}^X \right. \right. \\ \left. \left. - P_0(\mu_1)Q_{0\mu_1\mu_1}^X + P_0^2(\mu_1)Q_{\mu_100}^X + P_0^2(\mu_1)Q_{00\mu_1}^X + P_0^2(\mu_1)Q_{000}^X \right) - P_1^2(\mu_1)P_2(\mu_1) \left(Q_{\mu_2\mu_2\mu_2}^X \right. \right. \\ \left. \left. - P_0(\mu_2)Q_{\mu_2\mu_20}^X - P_0(\mu_2)Q_{\mu_20\mu_2}^X - P_0(\mu_2)Q_{0\mu_2\mu_2}^X + P_0^2(\mu_2)Q_{\mu_200}^X + P_0^2(\mu_2)Q_{0\mu_20}^X + P_0^2(\mu_2)Q_{00\mu_2}^X - P_0^3(\mu_2)Q_{000}^X \right) \right], \quad (45)$$

$$Y_{111}^{ZL} \geq \frac{1}{P_1^2(\mu_2)P_1^2(\mu_1)[P_2(\mu_2)P_1(\mu_1) - P_2(\mu_1)P_1(\mu_2)]} \left[P_1^2(\mu_2)P_2(\mu_2) \left(Q_{\mu_1\mu_1\mu_1}^Z - P_0(\mu_1)Q_{\mu_1\mu_10}^Z - P_0(\mu_1)Q_{\mu_10\mu_1}^Z \right. \right. \\ \left. \left. - P_0(\mu_1)Q_{0\mu_1\mu_1}^Z + P_0^2(\mu_1)Q_{\mu_100}^Z + P_0^2(\mu_1)Q_{00\mu_1}^Z + P_0^2(\mu_1)Q_{000}^Z \right) - P_1^2(\mu_1)P_2(\mu_1) \left(Q_{\mu_2\mu_2\mu_2}^Z \right. \right. \\ \left. \left. - P_0(\mu_2)Q_{\mu_2\mu_20}^Z - P_0(\mu_2)Q_{\mu_20\mu_2}^Z - P_0(\mu_2)Q_{0\mu_2\mu_2}^Z + P_0^2(\mu_2)Q_{\mu_200}^Z + P_0^2(\mu_2)Q_{0\mu_20}^Z + P_0^2(\mu_2)Q_{00\mu_2}^Z - P_0^3(\mu_2)Q_{000}^Z \right) \right], \quad (46)$$

$$e_{111}^{BZU} \leq \frac{1}{P_1^3(\mu_1)Y_{111}^{XL}} \left(E_{\mu_1\mu_1\mu_1}^Z Q_{\mu_1\mu_1\mu_1}^Z - P_0(\mu_1)E_{\mu_1\mu_10}^Z Q_{\mu_1\mu_10}^Z - P_0(\mu_1)E_{\mu_10\mu_1}^Z Q_{\mu_10\mu_1}^Z \right. \\ \left. - P_0(\mu_1)E_{0\mu_1\mu_1}^Z Q_{0\mu_1\mu_1}^Z + P_0^2(\mu_1)E_{\mu_100}^Z Q_{\mu_100}^Z + P_0^2(\mu_1)Q_{00\mu_1}^Z Q_{0\mu_10}^Z + P_0^2(\mu_1)E_{00\mu_1}^Z Q_{00\mu_1}^Z - P_0^3(\mu_1)E_{000}^Z Q_{000}^Z \right). \quad (47)$$

C. MDI-QSS with Quantum Non-demolition Measurement Technique

In this subsection, we perform MDI-QSS with weak coherent states by employing quantum non-demolition measurement technique. The density matrix of phase randomized weak coherent sources after channel transmission can be written as

$$\rho_3 = e^{-\mu\eta_t} \sum_{n=0}^{\infty} \frac{(\mu\eta_t)^n}{n!} |n\rangle\langle n|, \quad (48)$$

where the efficiency of channel transmission $\eta_t = 10^{-\beta L/10}$. David performs quantum non-demolition measurement on the three incoming pulses from Alice, Bob and Charlie before the pulses enter the GHZ state measurement device. Only when all the photon numbers of the three incoming pulses are no more than one, David will thereafter make a GHZ state measurement. Therefore, the gain $Q_{HHV}^{\mu\nu\omega\Phi_0^+}$ and the yield $Y_{nml}^{HHV\Phi_0^+}$ can be written as

$$Q_{HHV}^{\mu\nu\omega\Phi_0^+} = \frac{1}{8} \sum_{n=0}^1 \sum_{m=0}^1 \sum_{l=0}^1 e^{-\mu\eta_t - \nu\eta_t - \omega\eta_t} \frac{(\mu\eta_t)^n}{n!} \frac{(\nu\eta_t)^m}{m!} \frac{(\omega\eta_t)^l}{l!} Y_{nml}^{HHV\Phi_0^+},$$

$$Y_{nml}^{HHV\Phi_0^+} = \sum_{p=0}^{n+l} \sum_{s=0}^m \left[K_{1H}K_{2H}K_{3H}(1 - K_{1V})(1 - K_{2V})(1 - K_{3V}) + K_{1H}K_{2V}K_{3V}(1 - K_{1V})(1 - K_{2H})(1 - K_{3H}) \right. \\ \left. + K_{1V}K_{2H}K_{3V}(1 - K_{1H})(1 - K_{2V})(1 - K_{3H}) + K_{1V}K_{2V}K_{3H}(1 - K_{1H})(1 - K_{2H})(1 - K_{3V}) \right] P_{nml}^{HHV}, \quad (49)$$

where K_{1H} is the detection probability of detection mode $1H$, and

$$P_{nml}^{HHV} = \left| \sum_{t=0}^l \frac{(-1)^{l-t} C_n^{p-t} C_m^s C_l^t}{\sqrt{2^{n+m+l} n! m! l!}} \sqrt{p! s! (n+l-p)! (m-s)!} \right|^2, \quad (50)$$

$$K_{1H} = 1 - (1 - p_d)(1 - \eta_d)^s, \quad K_{1V} = 1 - (1 - p_d)(1 - \eta_d)^{m-s}, \quad K_{2H} = p_d,$$

$$K_{2V} = p_d, \quad K_{3H} = 1 - (1 - p_d)(1 - \eta_d)^p, \quad K_{3V} = 1 - (1 - p_d)(1 - \eta_d)^{n+l-p}.$$

The above methods can also be extended to cases of other polarizations. Similarly to the procedure above, one can calculate the parameters of Eq. (32). With the above two methods, we can obtain the numerical simulation results of the secure key rates of MDI-QSS (see Fig. 4).

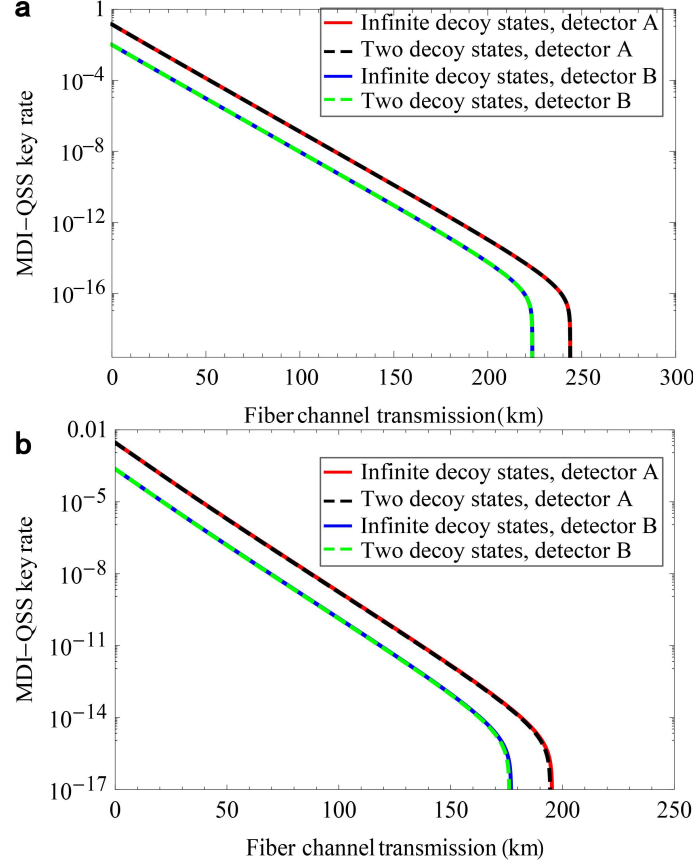


FIG. 4. (color online) Lower bound on the secure key rates versus fiber channel transmission. **a**, MDI-QSS with heralded single-photon sources. **b**, MDI-QSS with weak coherent sources based on quantum non-demolition measurement technique. We show the simulation results of infinite decoy states and two decoy states with detector A (B) of detection efficiency 93% (40%), respectively. The overall misalignment-error probability e_d of the system is 1.5%. The phase-randomized heralded single photon sources are used for MDI-QSS. The intensity of the signal state (one decoy state) is 5×10^{-3} (5×10^{-4}), while the other decoy state is a vacuum state. The phase-randomized weak coherent sources are used for MDI-QSS aided by quantum non-demolition measurement technique. The intensity of the signal state (one decoy state) is 0.4 (0.005), while the other decoy state is a vacuum state.

IV. MERMIN'S INEQUALITY

For tripartite systems, each particle is measured by Alice, Bob and Charlie with two bases (settings), local hidden-variable theories must obey Mermin's inequality [33]

$$M = \langle XXX \rangle - \langle XYY \rangle - \langle YXY \rangle - \langle YYX \rangle \leq 2, \quad (51)$$

where M is the Mermin value, and

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (52)$$

The Mermin value can reach the maximal value of 4 given that the tripartite GHZ states are measured under the ideal circumstance, e.g., for

$$|\Phi_0^+\rangle = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle). \quad (53)$$

Here, we combine the decoy-state method with weak coherent state sources to estimate the Mermin value of our post-selected GHZ states,

$$M_{111}^{\Phi_0^+} = \langle XXX \rangle_{111}^{\Phi_0^+} - \langle XYY \rangle_{111}^{\Phi_0^+} - \langle YXY \rangle_{111}^{\Phi_0^+} - \langle YYX \rangle_{111}^{\Phi_0^+}, \quad (54)$$

where $\langle XXX \rangle_{111}^{\Phi_0^+}$ is the expectation value of the GHZ state solely contributed by the single-photon state components, which results from the successful projection into the GHZ state $|\Phi_0^+\rangle$, given that Alice, Bob and Charlie send out the quantum states of X basis. The expectation value of $\langle XXX \rangle_{111}^{\Phi_0^+}$ is given by

$$\langle XXX \rangle_{111}^{\Phi_0^+} = (1 - 2e_d) \frac{Y_{+++}^{111\Phi_0^+} + Y_{+--}^{111\Phi_0^+} + Y_{-+-}^{111\Phi_0^+} + Y_{--+}^{111\Phi_0^+} - Y_{++-}^{111\Phi_0^+} - Y_{+-+}^{111\Phi_0^+} - Y_{-++}^{111\Phi_0^+} - Y_{---}^{111\Phi_0^+}}{Y_{+++}^{111\Phi_0^+} + Y_{+--}^{111\Phi_0^+} + Y_{-+-}^{111\Phi_0^+} + Y_{--+}^{111\Phi_0^+} + Y_{++-}^{111\Phi_0^+} + Y_{+-+}^{111\Phi_0^+} + Y_{-++}^{111\Phi_0^+} + Y_{---}^{111\Phi_0^+}}. \quad (55)$$

With weak coherent state sources, the gain $Q_{+++}^{\mu\nu\omega\Phi_0^+}$ and $Q_{---}^{\mu\nu\omega\Phi_0^+}$ can be written as

$$Q_{+++}^{\mu\nu\omega\Phi_0^+} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} Y_{+++}^{nml\Phi_0^+}, \quad Q_{---}^{\mu\nu\omega\Phi_0^+} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \sum_{l=0}^{\infty} \frac{\mu^n \nu^m \omega^l}{n!m!l!} e^{-\mu-\nu-\omega} Y_{---}^{nml\Phi_0^+}, \quad (56)$$

where $Y_{+++}^{nml\Phi_0^+}$ ($Y_{---}^{nml\Phi_0^+}$) is the yield given that Alice, Bob and Charlie send out n -photon state, m -photon state and l -photon state with $|+\rangle$ ($|-\rangle$) polarization, respectively. Thus we can obtain the lower (upper) bound of $Y_{+++}^{111\Phi_0^+L}$ ($Y_{+++}^{111\Phi_0^+U}$ and $Y_{---}^{111\Phi_0^+U}$) in the following,

$$Y_{+++}^{111\Phi_0^+L} \geq \frac{1}{\mu_2^3 \mu_1^3 (\mu_2 - \mu_1)} \left[\mu_2^4 \left(e^{3\mu_1} Q_{+++}^{\mu_1\mu_1\mu_1\Phi_0^+} - e^{2\mu_1} Q_{+++}^{\mu_1\mu_1 0\Phi_0^+} - e^{2\mu_1} Q_{+++}^{\mu_1 0\mu_1\Phi_0^+} - e^{2\mu_1} Q_{+++}^{0\mu_1\mu_1\Phi_0^+} + e^{\mu_1} Q_{+++}^{\mu_1 00\Phi_0^+} \right. \right. \\ \left. \left. + e^{\mu_1} Q_{+++}^{0\mu_1 0\Phi_0^+} + e^{\mu_1} Q_{+++}^{00\mu_1\Phi_0^+} - Q_{+++}^{000\Phi_0^+} \right) - \mu_1^4 \left(e^{3\mu_2} Q_{+++}^{\mu_2\mu_2\mu_2\Phi_0^+} - e^{2\mu_2} Q_{+++}^{\mu_2\mu_2 0\Phi_0^+} \right. \right. \\ \left. \left. - e^{2\mu_2} Q_{+++}^{\mu_2 0\mu_2\Phi_0^+} - e^{2\mu_2} Q_{+++}^{0\mu_2\mu_2\Phi_0^+} + e^{\mu_2} Q_{+++}^{\mu_2 00\Phi_0^+} + e^{\mu_2} Q_{+++}^{0\mu_2 0\Phi_0^+} + e^{\mu_2} Q_{+++}^{00\mu_2\Phi_0^+} - Q_{+++}^{000\Phi_0^+} \right) \right], \quad (57)$$

$$Y_{+++}^{111\Phi_0^+U} \leq \frac{1}{\mu_1^3} \left(e^{3\mu_1} Q_{+++}^{\mu_1\mu_1\mu_1\Phi_0^+} - e^{2\mu_1} Q_{+++}^{\mu_1\mu_1 0\Phi_0^+} - e^{2\mu_1} Q_{+++}^{\mu_1 0\mu_1\Phi_0^+} - e^{2\mu_1} Q_{+++}^{0\mu_1\mu_1\Phi_0^+} + e^{\mu_1} Q_{+++}^{\mu_1 00\Phi_0^+} \right. \\ \left. + e^{\mu_1} Q_{+++}^{0\mu_1 0\Phi_0^+} + e^{\mu_1} Q_{+++}^{00\mu_1\Phi_0^+} - Q_{+++}^{000\Phi_0^+} \right). \quad (58)$$

$$Y_{---}^{111\Phi_0^+U} \leq \frac{1}{\mu_1^3} \left(e^{3\mu_1} Q_{---}^{\mu_1\mu_1\mu_1\Phi_0^+} - e^{2\mu_1} Q_{---}^{\mu_1\mu_1 0\Phi_0^+} - e^{2\mu_1} Q_{---}^{\mu_1 0\mu_1\Phi_0^+} - e^{2\mu_1} Q_{---}^{0\mu_1\mu_1\Phi_0^+} + e^{\mu_1} Q_{---}^{\mu_1 00\Phi_0^+} \right. \\ \left. + e^{\mu_1} Q_{---}^{0\mu_1 0\Phi_0^+} + e^{\mu_1} Q_{---}^{00\mu_1\Phi_0^+} - Q_{---}^{000\Phi_0^+} \right). \quad (59)$$

From Eq. (22) and Eq. (56), we have

$$Y_{+++}^{111\Phi_0^+} = Y_{+--}^{111\Phi_0^+} = Y_{-+-}^{111\Phi_0^+} = Y_{--+}^{111\Phi_0^+}, \\ Y_{---}^{111\Phi_0^+} = Y_{+-+}^{111\Phi_0^+} = Y_{-++}^{111\Phi_0^+} = Y_{+++}^{111\Phi_0^+}. \quad (60)$$

The lower bound of $\langle XXX \rangle_{111}^{\Phi_0^+}$ can be given by

$$\langle XXX \rangle_{111}^{\Phi_0^+ L} = (1 - 2e_d) \frac{Y_{+++}^{111\Phi_0^+ L} - Y_{---}^{111\Phi_0^+ U}}{Y_{+++}^{111\Phi_0^+ U} + Y_{---}^{111\Phi_0^+ U}}. \quad (61)$$

Similar to the above methods, we have the expectation values of $\langle XYY \rangle_{111}^{\Phi_0^+}$, $\langle YXY \rangle_{111}^{\Phi_0^+}$ and $\langle YYX \rangle_{111}^{\Phi_0^+}$ as follows,

$$\langle XXX \rangle_{111}^{\Phi_0^+} = -\langle XYY \rangle_{111}^{\Phi_0^+} = -\langle YXY \rangle_{111}^{\Phi_0^+} = -\langle YYX \rangle_{111}^{\Phi_0^+}. \quad (62)$$

Therefore, the lower bound of the Mermin value can be given by

$$M_{111}^{\Phi_0^+ L} = 4\langle XXX \rangle_{111}^{\Phi_0^+ L} = 4(1 - 2e_d) \frac{Y_{+++}^{111\Phi_0^+ L} - Y_{---}^{111\Phi_0^+ U}}{Y_{+++}^{111\Phi_0^+ U} + Y_{---}^{111\Phi_0^+ U}}. \quad (63)$$

V. MERMIN'S THREE-PARTICLE VERSION OF THE KOCHEN-SPECKER THEOREM

The usual GHZ experiment goes by creating a (post-selected) GHZ entangled state and then sending each particle in the GHZ entanglement over a distance to Alice, Bob and Charlie, each of whom measures the received particle along a randomly chosen basis (either X basis or Y basis). Each of measured values for each observer should have a predetermined value and as such, Mermin's inequality like Eq. (4) in the main text necessarily follows, as required by local realism, which can be ruled out by performing the actual GHZ experiment.

However, the protocol for demonstrating the violation of Mermin's inequality is in some sense the time-reversed GHZ experiment, where the state preparations replace the state measurements in the usual GHZ test and the GHZ-entangled state is measured at the end of each run of the experiment, rather than prepared at the beginning of each run. The interpretation of such a time-reversed GHZ experiment and, in particular, its relevance to the test of (local) realism have never been considered in the literature to the best of our knowledge and are thus interesting in its own right.

While it is beyond the scope of the main text of the present paper to clarify the point, here we would like to argue that the proposed time-reversed GHZ experiment enables the test of a particular form of the Kochen-Specker theorem [34] as proposed by Mermin [35]. The usual Bell theorem (Bell's inequalities and the GHZ theorem) has three independent assumptions [36]: locality, realism and freedom of choices (namely, the experimental setting choices are truly random and free). However, in the proposed time-reversed GHZ experiment, we can suppose that Alice, Bob and Charlie prepare their own single-photon states randomly either in the X basis or in the Y basis; as a proof-of-principle argument, we do not use the weak coherent light sources to avoid the experimental complication caused by the non-ideal light sources. The three single photons are then subject to the GHZ measurement at David's station. The measurements and the preparations of these single photons cannot be spacelike-separated. Then we immediately see that the proposed time-reversed GHZ experiment does not test local realism. Instead, we argue that what it actually tests is the Kochen-Specker theorem as proposed by Mermin for the case of eight-dimensional space of three spins/qubits [35].

The Kochen-Specker theorem states that quantum mechanical predictions for any systems of dimensions 3 or higher cannot be reproduced by noncontextual hidden-variable theories that assume the measurement results to be predetermined and independent of other compatible measurements. In Mermin's argument of the Kochen-Specker theorem, one makes use of a set of the operator identities:

$$\begin{aligned} X_1 X_2 X_3 \cdot X_1 \cdot X_2 \cdot X_3 &= 1, \\ X_1 Y_2 Y_3 \cdot X_1 \cdot Y_2 \cdot Y_3 &= 1, \\ Y_1 X_2 Y_3 \cdot Y_1 \cdot X_2 \cdot Y_3 &= 1, \\ Y_1 Y_2 X_3 \cdot Y_1 \cdot Y_2 \cdot X_3 &= 1, \\ X_1 X_2 X_3 \cdot X_1 Y_2 Y_3 \cdot Y_1 X_2 Y_3 \cdot Y_1 Y_2 X_3 &= -1, \end{aligned} \quad (64)$$

where (\cdot) is used to separate operators or operator products. Mermin's argument of the Kochen-Specker theorem is a state-independent proof. In the present time-reversed GHZ experiment, we only identify one $(|\Phi_0^+\rangle)$ out of the eight

GHZ states. Thus, for quantum mechanics to interpret the experiment, we have the following eigenequations

$$\begin{aligned}
X_1 X_2 X_3 \cdot X_1 \cdot X_2 \cdot X_3 |\Phi_0^+\rangle &= |\Phi_0^+\rangle, \\
X_1 Y_2 Y_3 \cdot X_1 \cdot Y_2 \cdot Y_3 |\Phi_0^+\rangle &= |\Phi_0^+\rangle, \\
Y_1 X_2 Y_3 \cdot Y_1 \cdot X_2 \cdot Y_3 |\Phi_0^+\rangle &= |\Phi_0^+\rangle, \\
Y_1 Y_2 X_3 \cdot Y_1 \cdot Y_2 \cdot X_3 |\Phi_0^+\rangle &= |\Phi_0^+\rangle, \\
X_1 X_2 X_3 \cdot X_1 Y_2 Y_3 \cdot Y_1 X_2 Y_3 \cdot Y_1 Y_2 X_3 |\Phi_0^+\rangle &= -|\Phi_0^+\rangle.
\end{aligned} \tag{65}$$

How to interpret Eq. (65) by noncontextual hidden-variable theories? According to Mermin [35], each of operators or operator products (denoted by O) separated by (\cdot) can be assigned a predetermined value $v(O)$. Thus the noncontextual hidden-variable theories predict the following relations among these predetermined values:

$$\begin{aligned}
v(X_1 X_2 X_3) v(X_1) v(X_2) v(X_3) &= 1, \\
v(X_1 Y_2 Y_3) v(X_1) v(Y_2) v(Y_3) &= 1, \\
v(Y_1 X_2 Y_3) v(Y_1) v(X_2) v(Y_3) &= 1, \\
v(Y_1 Y_2 X_3) v(Y_1) v(Y_2) v(X_3) &= 1, \\
v(X_1 X_2 X_3) v(X_1 Y_2 Y_3) v(Y_1 X_2 Y_3) v(Y_1 Y_2 X_3) &= -1.
\end{aligned} \tag{66}$$

Since $v(O) = \pm 1$, multiplying both sides of Eq. (66) yields $+1 = -1$, which is a conflict. The conflict implies that it is impossible to interpret the experiment by assuming the predetermined values to these operators or operator productions.

There is a trick that the predetermined values of the four operator productions, $v(X_1 X_2 X_3)$, $v(X_1 Y_2 Y_3)$, $v(Y_1 X_2 Y_3)$ and $v(Y_1 Y_2 X_3)$, appear either separately in the first to fourth lines of Eq. (66), or jointly in the last line of Eq. (66). For the above argument to be valid, either one has to make an additional assumption (e.g., measurements of the four operator productions do not disturb each other) or one has to be able to measure the four operator productions with the same apparatus. A similar argument is essential in a GHZ-like refutation of local realism using two-photon hyperentanglement [37]. Fortunately, in the present case we can avoid the additional assumption also by measuring the four operator productions by the same apparatus, which is exactly the apparatus for the GHZ-state measurement.

The above reasoning is valid for ideal cases, namely, one has $v(O) = \pm 1$ exactly and perfect detections. For practical experiments, we have Mermin's inequality (51) by noting that we only identify $|\Phi_0^+\rangle$ out of the eight GHZ states.

As we noted in Section I.B, in the security proof of our multiparty quantum communication protocols, we suppose that each of Alice, Bob and Charlie has an EPR entangled state which contains one virtual qubit in each of them and the “signal” qubit is sent to the middle node, David. After a successful GHZ-state measurement performed by David, the virtual qubit of the legitimate users becomes a GHZ-entangled state. This procedure is known as a multiparty entanglement swapping. If we suppose that each of Alice, Bob and Charlie possesses two EPR-entangled photons, rather than the virtual+signal qubits, a successful GHZ-state measurement by David would result in three-photon GHZ entanglement. The GHZ entanglement created this way can be used to demonstrate the violation of local realism as usual provided that the measurements performed by Alice, Bob, Charlie and David are spacelike separated. Such an experiment can even be performed in a delayed-choice version, as demonstrated for the case of two qubits both theoretically [38] and experimentally [39].

* zbchen@ustc.edu.cn

- [1] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [2] E. N. Maneva and J. A. Smolin, Contemp. Math. **305**, 203 (2002).
- [3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [4] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).
- [5] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
- [6] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
- [7] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
- [8] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
- [9] B. M. Terhal, IBM J. Research and Development **48**, 71 (2004).
- [10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

- [11] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
- [12] J.-W. Pan and A. Zeilinger, Phys. Rev. A **57**, 2208 (1998).
- [13] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
- [14] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
- [15] C.-Y. Lu, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **103**, 020501 (2009).
- [16] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
- [17] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
- [18] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [19] P. Grangier, J. Levenson, and J. Poizat, Nature **396**, 537 (1998).
- [20] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
- [21] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).
- [22] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
- [23] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).
- [24] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014).
- [25] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
- [26] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
- [27] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, et al., Phys. Rev. Lett. **111**, 130502 (2013).
- [28] S.-B. Cho and T.-G. Noh, Opt. Express **17**, 19027 (2009).
- [29] Y. Liu, L. Ju, X.-L. Liang, S.-B. Tang, G.-L. S. Tu, L. Zhou, C.-Z. Peng, K. Chen, T.-Y. Chen, Z.-B. Chen, et al., Phys. Rev. Lett. **109**, 030501 (2012).
- [30] A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, and G. Xavier, Nature Commun. **4**, 2871 (2013).
- [31] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).
- [32] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
- [33] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [34] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).
- [35] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
- [36] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, et al., Proc. Natl. Acad. Sci. **107**, 19708 (2010).
- [37] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, Č. Brukner, and A. Zeilinger, Phys. Rev. Lett. **90**, 160408 (2003).
- [38] A. Peres, J. Mod. Opt. **47**, 139 (2000).
- [39] X.-S. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, Nature Phys. **8**, 479 (2012).